BY ORDER OF THE SECRETARY OF THE AIR FORCE

AIR FORCE INSTRUCTION 16-1406

25 AUGUST 2015

AIR FORCE MATERIEL COMMAND Supplement

3 JUNE 2016

Operations Support

AIR FORCE INDUSTRIAL SECURITY PROGRAM

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

ACCESSIBILITY: Publications and forms are available at **www.e-Publishing.af.mil** for downloading or ordering on the e-Publishing website

RELEASABILITY: There are no releasability restrictions on this publication

OPR: SAF/AAZ

Certified by: SAF/AAZ (Mr. David Lowy)

Pages: 48

Supersedes: AFI31-601, June 29, 2005

(AFMC)

OPR: HQ AFMC/IP

Certified by: HQ AFMC/IP (Mr David D Day)

Pages:17

Supersedes: AFI 31-601_AFMCSUP, 31 March 2010

This publication implements the industrial security portion of the Security Enterprise defined in Air Force Policy Directive (AFPD) 16-14, *Security Enterprise Governance*. It provides guidance for implementing the National Industrial Security Program and is applicable to AF personnel, the Air National Guard, the Air Force Reserve, and DoD contractors performing under the terms of a properly executed contract and associated visitor group security agreement as determined appropriate by the serivicing installation commander. This may include access to Controlled Unclassified Information (CUI), and technical information as defined in DFARS clause 252.204-7012, *Safeguarding of Unclassified Controlled Technical Information*. Use this instruction with DoD 5220.22-R, *Industrial Security Regulation,* DoD 5220.22-M, *National Industrial Security Program: Procedures for Government Activities Relating to Foreign Ownership, Control, or Influence (FOCI)*: *Volume* 3, and DoD 5200.01-M V1-4, *DoD Information Security Program* and if necessary, DoD 5220.22-M, *National Industrial Security Program Operating Manual (NISPOM)*. Ensure records created as a result of processes prescribed in this publication are

maintained IAW Air Force Manual (AFMAN) 33-363, *Management of Records* and disposed of IAW the Air Force Records Disposition Schedule (RDS) in the Air Force Records Information Management System (AFRIMS). Refer recommended changes and questions about this publication to the Office of Primary Responsibility (OPR) using the AF Form 847, Recommendation for Change of Publication; route AF Forms 847 from the field through the appropriate functional chain of command. This publication may be supplemented by MAJCOM but drafts must be reviewed by this publication's OPR prior to publishing. (T-1) The authorities to waive wing/unit level requirements in this publication are identified with a Tier ("T-0, T-1, T-2, T-3") number following the compliance statement.

(AFMC) This instruction extends the guidance of AFI 16-1406, *Air Force Industrial Security Program*. This supplement replaces AFI 31-601_AFMC Supplement; change includes addition of Center responsibilities and clarification of National Interest Determination (NID) policy. This supplement is applicable to Air Force Reserve Command units and personnel tenant on AFMC Installations. This publication does not apply to the Air National Guard. This publication may be supplemented at any level. Refer recommended changes and questions about this publication to the Office of Primary Responsibility (OPR) using AF Form 847, *Recommendation for Change of Publication*; route AF Forms 847 from the field through the appropriate functional chain of command to HQ AFMC/IP. Submit written requests for clarification to this supplement to HQ AFMC/IP. The authorities to waive wing/unit level requirements in this publication are identified with a Tier ("T-0, T-1, T-2, T-3") number following the compliance statement. See AFI 33-360, *Publications and Forms Management*, for a description of the authorities associated with the Tier numbers. Submit requests for waivers through the chain of command to the appropriate Tier waiver approval authority, or alternately, to the Publication OPR for non-tiered compliance items. Ensure that all records created as a result of processes prescribed in this publication are maintained in accordance with (IAW) Air Force Manual (AFMAN) 33-363, *Management of Records*, and disposed of IAW Air Force Records Information Management System (AFRIMS) Records Disposition Schedule (RDS).

Chapter 1

PROGRAM OVERVIEW AND ROLES AND RESPONSIBILITIES

1.1. AF Security Enterprise. AFPD 16-14 defines the Air Force Security Enterprise as the organizations, infrastructure, and measures (policies, processes, procedures, and products) in place to safeguard AF personnel, information, operations, resources, technologies, facilities, and assets against harm, loss, or hostile acts and influences. Information Protection is a subset of the Air Force Security Enterprise. Air Force Industrial Security is a core discipline within Information Protection.

1.2. Information Protection. Information Protection is a subset of the Air Force Security Enterprise. Information Protection consists of three core security disciplines (Personnel, Industrial, and Information Security) which support insider threat detection and mitigation efforts and are used to:

1.2.1. Determine military, civilian, and contractor personnel eligibility to access classified information (Personnel Security).

1.2.2. Ensure the protection of classified and CUI information released or disclosed to industry in connection with classified contracts (Industrial Security).

1.2.3. Protect classified information and CUI that, if subject to unauthorized disclosure, could reasonably be expected to cause damage to national security (Information Security).

1.3. Information Protection Oversight. These key positions direct, administer, and oversee management, functioning and effectiveness of the Information Protection Program.

1.3.1. The Senior Agency Official (SAF/AA) is the Secretary of the Air Force appointed authority responsible for the oversight of Information Protection.

1.3.2. The Security Program Executive (SPE) is appointed by the MAJCOM/DRU Commander in accordance with AFPD 16-14 and is responsible oversight of Information Protection for their MAJCOM/DRU.

1.3.2. **(AFMC)** AFMC/CV is the AFMC SPE.

1.3.2.1. **(Added-AFMC)** Center CVs are the Center's SPE. **(T-2).**

1.3.3. Wing Commanders provide oversight of Information Protection by ensuring security controls, safeguards, and countermeasures are established through application of risk management principles, as appropriate, for their wings. (T-1) This may be delegated to the Wing/CV.

1.3.3. **(AFMC)** This also applies to the 66 ABG Commander and Arnold Engineering Development Complex (AEDC) Commander.

1.3.3.1. **(Added-AFMC)** Oversight provided to units/organizations outside the ABW/TW/ABG/AEDC will be defined in host tenant support agreements, Memorandum of Understanding (MOU), Memorandum of Agreement (MOA), or Center supplement in accordance with AFI 25-201. **(T-2).**

1.4. Information Protection Managers. These key positions develop guidance as necessary, and serve as principal advisors to the personnel identified in paragraph 1.3.

1.4.1. Director of Security, Special Program Oversight and Information Protection (SAF/AAZ) is responsible to the Senior Agency Official and addresses the equities within the functional portfolio related to Information Protection.

1.4.2. MAJCOM/DRU Director, Information Protection is responsible to the SPE and for integrating Information Protection into MAJCOM/DRU operations and provides oversight and direction to the security specialists and other personnel assigned to the MAJCOM/DRU Information Protection Directorate.

1.4.2. **(AFMC)** HQ AFMC/IP is AFMC's Director, Information Protection.

1.4.2.1. **(Added-AFMC)** The Center CV is responsible for assigning a Center Chief, Information Protection (CIP) responsible for advising the Center in Information Protection (IP) policy and processes. The Center CIP may be dual-hatted as the Wing CIP or organizationally aligned elsewhere within the Center as determined by the Center/CV. Center CIPs will coordinate with Wing CIPs at all locations where the Center has organizations to ensure IP support requirements are agreed upon and delegated appropriately through host tenant support agreements, MOU, MOA, formal Center-to-Center level agreements, or Center supplement in accordance with AFI 25-201. **(T-2).**

1.4.3. Chief, Information Protection is responsible for executing Information Protection on behalf of the Wing Commander and provides oversight and direction to commanders and directors at all levels and their security managers, and security specialists and other personnel assigned to the DRU/Wing Information Protection Office. (T-1)

1.4.3. **(AFMC)** Air Base Wing/Test Wing (including 66 ABG and AEDC) IP office is the Wing CIP. The Wing CIP provides support and oversight to all organizations within the Wing, to include all tenant organizations when required by a host tenant support agreement, MOU, MOA, formal Center-to-Center level agreements, or Center supplement in accordance with AFI 25-201. **(T-2).**

1.4.3.1. **(Added-AFMC)** The Center CIP serves as the interface with MAJCOM and Center leadership in the development and implementation of IP policy and procedures across the Center.

1.4.4. Commanders and Directors ensure military and civilian personnel are properly cleared for access to classified information and CUI, integrate contractors into their existing security programs, and protect classified information and CUI under their authority to support Information Protection. (T-1)

1.4.4. **(AFMC)** Commanders and Directors perform these duties at all locations under their command to include geographically separated units (GSU). If authorized, Commanders and Directors may delegate duties at GSUs to the GSU's lead position (e.g., Division, Branch Chiefs). **(T-2).**

1.5. Information Protection Implementation. The key security professionals below are responsible for implementing Information Protection core security disciplines (information, industrial, and personnel security):

1.5.1. Security Specialists are Office of Personnel Management (OPM) occupational series 0080, Security Administration, and are responsible for effecting Information Protection core

security disciplines (Information, Personnel, Industrial Security) for a MAJCOM/DRU, or Wing.

1.5.1.1. **(Added-AFMC)** At a Center, Security Specialists that manage the Center's Information Protection program are normally assigned to the IP Office and report to the Center CIP.

1.5.1.2. **(Added-AFMC)** Security Specialists are also assigned within other organizations and perform functions which incorporate the core security disciplines into unique organizational missions such as research, development, acquisition, and test activities.

1.5.2. Security Managers are principal advisors to commanders and directors. They implement the core security disciplines under the guidance and direction of the DRU/Wing Chief, Information Protection or one of the security specialists assigned to the Information Protection Office.

1.5.2.1. **(Added-AFMC)** For Centers with GSUs located at other Center and/or MAJCOM locations, the Center CIP is responsible for developing and formalizing organizational responsibility for guidance, direction, and oversight of GSU security manager programs. The intent is to ensure each unit security manager program is provided support and oversight on a consistent and continual basis. **(T-2).**

1.5.3. Military or civil service personnel assigned to the Information Protection Directorate or Office must meet the rank/grade requirements listed in DoD 5200.01-M, Volume 1, Enclosure 2, and complete training equivalent to information security specialists as prescribed in AFI 16-1404. (T-1)

1.6. Industrial Security. This core security discipline of Information Protection is designed to identify and protect classified national security information within DoD when that information is entrusted to industry. In most cases for the AF, "industry" consists of contractors that have been validated by DSS to have access to classified material. This AFI is used in conjunction with AFI 16-1404, Air Force *Information Security Program*. Within the AF industrial security program:

1.6.1. Identify in classified contracts using the DoD Contract Security Classification Specification (referred to as DD Form 254) procedures for protection of classified information/sensitive resources.

1.6.1. **(AFMC)** A DD Form 254 form will be included with the Request for Bid, Request for Proposal, Request for Information to clarify security requirements for the final contract award. When access to classified information is required during the acquisition process, a DD Form 254 shall be completed in the same manner as a DD Form 254 for awarding a contract. See AFI 16-1406 Chapter 3. **(T-2).**

1.6.2. Categorize on-site contractors as Vistor Groups and integrate contractors into the organization's information security program in accordance with this AFI and AFI 16-1404.

1.6.2. **(AFMC)** Integrate contractor operations, performed on an AF installation, into the installation or Centers Information Security Program unless mission or performance requirements demand contractor groups to be designated as NISPOM visitor groups. The CIP will evaluate NISPOM visitor groups under the NISPOM, the contract requirements, and

visitor group security agreement (VGSA) requirements. This should be the exception not the rule. **(T-2).** See Terms for **NISPOM Visitor Group**.

1.6.3. When the installation commander has elected to retain security cognizance of contractors as cleared facilities, conduct security reviews in accordance with the NISPOM. NOTE: Categorize DoD contractor operations supporting the AF overseas as visitor groups.

1.6.3. **(AFMC)** When security cognizance is retained for cleared facilities on an AF installation, the host-installation cybersecurity office (formerly information assurance) will assist the servicing CIP by providing oversight to the contractor's system/networks that process/store Government information to ensure those system/networks are properly accredited and all DoD/AF information technology cybersecurity requirements are met. **(T-2).**

1.6.4. Defense Secruity Service (DSS) makes risk management determinations for the AF relating to contractor Foreign Ownership, Control, or Influence (FOCI) to include National Interest Determination (NID) when needed.

1.6.4. **(AFMC)** See DoDM 5220.22, Volume 3, National Industrial Security Program: Procedures for Government Activities Relating to Foreign Ownership, Control or Influence (FOCI) and DTM 15-002, Policy Guidance for the Processing of National Interest Determinations in Connection with FOCI.

1.6.5. Only contracting offices award or modify contracts. Once awarded or modified, notify the servicing Wing Information Protection Office as soon as possible, but not to exceed 30 days of award or modification. (T-1)

1.6.5. **(AFMC)** Contracting Officer, with assistance from the Program Manager and Unit Security Manager, notifies the servicing IP Offices at all contract performance locations when a contract requiring performance on a Government installation and access to classified information is awarded or modified. For assistance in identifying which servicing IP office, contact local servicing IP office.

1.7. Other Roles and Responsibilities. A key stakeholder contributing to an effective AF industrial security posture among those identified in AFI 16-1404 is:

1.7.1. The Deputy Assistant Secretary (Contracting), Assistant Secretary (Acquisition), (SAF/AQC) is responsible for formulating and interpreting contracting policy and issuing supplemental guidance to the FAR. Administrative Contracting Officers (ACO) and Procuring Contracting Officers (PCO) are key players within the contracing community; contracting office (CO) is used throughout this instruction to denote those responsibilities regardless of ACO or PCO actions at all levels.

Chapter 2

INDUSTRIAL SECURITY IMPLEMENTATION

2.1. Security Program Executives (SPE). In addition to duties found in AFI 16-1404, provide oversight of industrial security program activites within their area of responsibility.

2.1.1. Approve program waivers and exceptions to policy and submit them to SAF/AA, when necessary.

2.1.1. **(AFMC)** Wing CIPs will submit waivers and exception to policy requests to Center/IP through their Wing/CV. Center CIPs will submit waivers and exception to policy requests to HQ AFMC/IP through their Center/CV. HQ AFMC/IP will submit waivers and exception to policy requests through AFMC/CV to SAF/AAZ. **(T-2).**

2.1.2. Assess reports concerning espionage, sabotage, subversive activities, deliberate compromises of classified information, and leaks of classified information to the media involving cleared facilities or visitor groups and determine appropriate risk based countermeasures. Submit reports to SAF/AA.

2.1.2. **(AFMC)** Center CIPs will submit reports to HQ AFMC/IP through their Center/CV. HQ AFMC/IP will submit reports through AFMC/CV to SAF/AAZ. **(T-2).**

2.2. MAJCOM/DRU Director, Information Protection. In addition to AFI 16-1404 responsibilities for Information Security, ensures Industrial Security Program implementation and provides oversight of subordinate Wings or organizations within their area of operations.

2.2. (AFMC)MAJCOM/DRU Director, Information Protection. Provide oversight of subordinate Centers. **(T-2).**

2.2.1. Assess program waivers and exceptions to policy and validate their accuracy prior to submission to the SPE for approval.

2.2.2. Provide the SPE risked-based countermeasure strategies concerning reported espionage, sabotage, subversive activies, deliberate compromises of classified information, and leaks of classified information to the media involving cleared facilities and visitor groups located on or serviced by the command.

2.2.3. Develop industrial security data calls or responses when requested.

2.2.4. Ensure industrial security supplements and self-assessment checklists are coordinated with SAF/AAZ prior to publication and submission to the Management Internal Control Tool (MICT) database.

2.2.5. Notify SAF/AAZ of unsatisfactory Security Reviews of cleared facilities.

2.2.6. Report security violations and infraction metrics to SAF/AAZ when requested.

2.3. MAJCOM/DRU Industrial Security Specialist. Works closely with the MAJCOM/DRU Information Security Specialist to deliver a robust Industrial Security Program for the command.

2.3.1. Research program standards to validate program waivers and exceptions.

2.3.2. Participate in the development of risk based countermeasure strategies for reports concerning espionage, sabotage, subversive activities, deliberate compromises of classified

information, and leaks of classified information to the media involving cleared facilities or visitor groups and determine appropriate risk based countermeasures.

2.3.3. Collect data to support industrial security data calls when requested.

2.3.4. Write and develop industrial security supplements and self-assessment checklists.

2.3.5. Notify the Director, Information Protection of unsatisfactory security reviews of cleared facilities.

2.3.6. Track unsatisfactory security reviews of cleared facilities until deficiencies are corrected or administrative action is taken on the Facility Security Clearance (FCL).

2.3.7. Collect, analyze and maintain metrics for security violations and infractions.

2.3.7. **(AFMC)** AFI 16-1406, paragraph 2.3.7 only applies to security incidents caused by contractors working for integrated or NISPOM visitor groups.

2.3.8. Process contractor reported security violations to SAF/AAZ. Upon receipt from SAF/AAZ, these are distributed to the appropriate Wing Information Protection Office.

2.3.8. **(AFMC)** HQ AFMC/IP will distribute to appropriate Center CIP. **(T-2).**

2.3.8.1. Process copies of replies to DSS to SAF/AAZ.

2.3.8.1. **(AFMC)** Copies for SAF/AAZ will go through HQ AFMC/IP. **(T-2).**

2.3.9. Submit National Interest Determinations (NID) to SAF/AAZ through Information Protection channels.

2.3.9. **(AFMC)** When a company requires a NID, the Contracting Officer with the assistance of the Program Manager and Unit Security Manager will send a NID request to DSS; see **Attachment 2**. When access to AF Top Secret (TS) information is required, DSS will need approval for collateral TS information from the original classification authority (OCA); see **Attachment 4** for a sample OCA TS NID request package. SAP NID requests will be processed through SAP channels. SCI NID requests will be processed through the supporting SSO to HQ AFMC/A2S. **(T-2).** Contact your servicing CIP for questions on collateral NID process. Contact HQ AFMC/A5/8Z, servicing Government SAP Security Officer (GSSO), or program security officer (PSO) for questions on SAP NIDs. Contact the servicing SSO for questions on SCI NIDs. DSS NID office is Defense Security Service FOCI Operations Division, (571) 305-6306 or **nid@dss.mil.** DoD reference for NIDs see DoDM 5220.22, Volume 3, National Industrial Security Program: *Procedures for Government Activities Relating to Foreign Ownership, Control or Influence (FOCI)* and DTM 15-002, *Policy Guidance for the Processing of National Interest Determinations in Connection with FOCI*.

2.3.9.1. Refer Special Access Program (SAP) NID questions/submissions to MAJCOM SAP Management Office.

2.3.9.1. **(AFMC)** AFMC SAP Management Office is HQ AFMC/A5/8Z.

2.4. Installation Commanders. In addition to responsibilities found in AFI 16-1404 for Wing Commanders and when the Installation Commander has elected to retain security cognizance of contractor facilities:

2.4.1. Submit program waivers and exceptions to policy to the SPE through Information Protection channels. (T-1)

2.4.1. **(AFMC)** Information Protection channels are defined as Wing CIP to Center CIP to HQ AFMC/IP; HQ AFMC/IP will interface with SAF/AAZ. Wing CIPs will submit waivers and exception to policy requests to Center/IP through their Wing/CV. Center CIPs will submit waivers and exception to policy requests to HQ AFMC/IP through their Center/CV. HQ AFMC/IP will submit waivers and exception to policy requests through AFMC/CV to SAF/AAZ. **(T-2).**

2.4.2. Provide reports concerning espionage, sabotage, subversive activities, deliberate compromises of classified information, and leaks of classified information to the media involving cleared facilities or visitor groups to the SPE, and determine risk based countermeasures to be enacted. (T-1)

2.4.2. **(AFMC)** Center CIPs will submit reports to HQ AFMC/IP through their Center/CV. HQ AFMC/IP will submit reports through AFMC/CV to SAF/AAZ. **(T-2).**

2.4.3. Grant contractors access to the installation.

2.4.3. **(AFMC)** This includes prime contractors and subcontractors.

2.4.4. Designate classified contractor operations as cleared facilities, visitor groups, or intermittent visitors. (T-1)

2.4.4. **(AFMC)** This includes prime contractors and subcontractors. The Installation Commander may delegate to the Installation CIP authority to designate classified contractor operations as intermittent visitors, integrated visitor groups, or NISPOM visitor groups in writing. The CIP will obtain Installation Commander's approval for cleared facilities. **(T-2).**

2.4.5. Enter into security agreements with contractors by signing Visitor Group Security Agreements (VGSA). (T-1) This may be delegated to the Chief, Information Protection.

2.4.5. **(AFMC)** This includes prime contractors and subcontractors. For subcontractors see paragraph **4.2.2**.

2.4.5.1. **(Added-AFMC)** Installation Commanders may elect to delegate signing VGSAs to a tenant CIP in writing through a memorandum, host tenant support agreements, MOU, MOA, or Installations supplement. Cleared facilities will be approved by the Installation Commander. **(T-2).**

2.5. (Wing) Chief, Information Protection. In addition to responsibilities found in AFI 16-1404, this position should establish rapport with program or project managers and commanders/directors (hereinafter referred to as program/project managers) to ensure effective management of the industrial security program. When the Installation Commander has elected to retain security cognizance of industrial security activities ensure the following:

2.5. (AFMC)Chief, Information Protection. These duties are also performed by the Center CIP at the Center level. Although some of the duties would require delegation by the Installation Commander for the Center CIP to perform.

2.5.1. Analyze and submit program waiver and exception packages through Information Protection channels to appropriate approval authority. (T-1)

2.5.1. **(AFMC)** Wing CIPs will submit waivers and exception to policy requests to Center/IP through their Wing/CV. Center CIPs will submit waivers and exception to policy requests to HQ AFMC/IP through their Center/CV. HQ AFMC/IP will submit waivers and exception to policy requests through AFMC/CV to SAF/AAZ. **(T-2).**

2.5.2. Brief the Installation Commander on reports concerning espionage, sabotage, subversive activities, deliberate compromises of classified information, and leaks of classified information to the media involving cleared facilities, visitor groups, or intermittent visitors and recommends appropriate risk based countermeasures. (T-1)

2.5.2. **(AFMC)** If Installation Commander delegated oversight to a tenant CIP, this delegated CIP will brief the host installation CIP and Installation Commander. **(T-2).**

2.5.3. Make recommendations to the Installation Commander on restricting access to classified information when security reviews result in an unsatisfactory rating. (T-1)

2.5.3. **(AFMC)** Pertaining to cleared facilities on AF installations; if the Installation Commander delegated oversight to a tenant CIP, this delegated CIP will brief the host installation CIP and Installation Commander of the unsatisfactory rating. CIPs will also coordinate recommendations with the AF sponsoring organization (i.e., Program Executive Officer/Manager, Contracting Officer, Contracting Officer's Representative, security specialist and other security disciplines as applicable.) **(T-2).**

2.5.3.1. If the cleared facility fails to take corrective actions, provide support information with recommendations (e.g., removal of facility clearance level). (T-1)

2.5.3.2. Notify the MAJCOM/DRU Director, Information Protection of facility rating. (T-1)

2.5.3.2. **(AFMC)** Notify HQ AFMC/IP through the Center CIP. **(T-2).** Also notify the AF Sponsoring Organization, Government Contracting Activity, Contracting Officer's Representative, Security Specialists and other security disciplines as applicable.

2.5.4. Develop staff packages to designate contractor operations as cleared facilities, visitor groups or intermittent visitors. This designation is determined by the visitor's relationship and interface with the AF activity and/or installation. (T-1)

2.5.5. Review VGSA and submit package to Installation Commander for signature unless this signature authority is delegated to the Chief of Information Protection. (T-1)

2.5.6. Serve as the authority to perform industrial security program oversight for contractor operations and coordinate with DSS when unique or special operational circumstances warrant. (T-1)

2.5.7. Coordinate with the MAJCOM/DRU Director, Information Protection, local contracting officer, and Home Office Facility (HOF) Facility Security Office (FSO) when assigning an unsatisfactory review rating for a cleared facility. (T-0)

2.5.8. Forward a copy of the security review and survey reports and other applicable documentation, pertaining to a "cleared facility" per DOD 5220.22-M, DOD 5220.22-R, and this instruction, as required to DSS. Forward a copy to the MAJCOM/DRU and SAF/AAZ through Information Protection channels when requested. (T-0)

2.5.8. **(AFMC)** Forward a copy to HQ AFMC/IP through the Center CIP. HQ AFMC/IP will forward the copy to SAF/AAZ. **(T-2).**

2.5.9. Administer, and ensure a copy of the returned response is provided by program/project managers to SAF/AAZ concerning DSS reported contractor security violations. (T-1)

2.5.9. **(AFMC)** Original Classification Authorities are responsible for conducting damage assessments in accordance with DODM 5200.01 Vol. 3, Encl. 6 and AFI 16-1404. Copy of response will be sent through the Center CIP to HQ AFMC/IP. HQ AFMC/IP will send the response to SAF/AAZ. **(T-2).**

2.5.10. Process NID requests through Information Protection channels to SAF/AAZ. Refer SAP NID questions/submissions to the appropriate MAJCOM SAP Management Office. (T-0)

2.5.10. **(AFMC)** When a company requires a NID, the Contracting Officer with the assistance of the Program Manager and Security Manager will send a NID request to DSS; see Attachment 2. When access to AF TS information is required, DSS will need approval for collateral TS information from the OCA; see **Attachment 4** for a sample OCA TS NID request package. SAP NID requests will be processed through SAP channels. SCI NID requests will be processed through the supporting SSO to HQ AFMC/A2S. **(T-2).** Contact your servicing CIP for questions on collateral NID process. Contact HQ AFMC/A5/8Z, servicing GSSO, or PSO for questions on SAP NIDs. Contact the servicing SSO for questions on SCI NIDs. DSS NID office is Defense Security Service FOCI Operations Division, (571) 305-6306 or **nid@dss.mil.** DoD reference for NIDs see DoDM 5220.22, Volume 3 and DTM 15-002.

2.6. (Wing) Industrial Security Specialist. Provide guidance to program/project managers (see para 2.5) to ensure security procedures (e.g., SCI, physical, OPSEC, SAP, etc.) are followed throughout the contracting process. Assist in determining the relationship and interface between the contractor and the Air Force to designate contractor activities as visitor group, cleared facility, or intermittent visitor. Work closely with the Wing Information Security Specialist to deliver a robust Industrial Security Program.

2.6. (AFMC)Industrial Security Specialist. These duties are also performed by the Center Industrial Security Specialist at the Center level. Although some of the duties would require delegation by the Installation Commander for the Center Industrial Security Specialist to perform.

2.6.1. When the Installation Commander has elected to retain security cognizance of contractor cleared facilities:

2.6.1.1. Review and prepare program waivers and exceptions to policy and develop staff packages for the commander. (T-1)

2.6.1.2. Analyze reports concerning espionage, sabotage, subversive activities, deliberate compromises of classified information, and leaks of classified information to the media involving cleared facilities, visitor groups, or intermittent visitors and develop possible courses of action to mitigate risks. (T-1)

2.6.1.3. Conduct industrial security reviews of cleared facilities in accordance with NISPOM. Collaborate with FSO to determine or monitor any necessary corrective actions. (T-1)

2.6.1.3. **(AFMC)** The servicing host-installation Cybersecurity (formerly information assurance) official will accompany the industrial security specialist to review the contractor's system/networks that process classified or controlled unclassified information for compliance. **(T-2).**

2.6.1.4. Staff correspondence for unsatisfactory ratings of security reviews. (T-1)

2.6.2. Establish a process with the servicing CO to ensure Information Protection Office is notified 30 days prior to work performance start date. (T-1)

2.6.2. **(AFMC)** Required when contract performance is on the IP's installation and access to classified information is required.

2.6.3. Participate in development of Visitor Group Security Agreements in accordance with Chapter 4, incorporating visitor groups into the serviced unit information security program. (T-1)

2.6.4. Review DD Form 254. Refer to Chapter 3 for specific guidance. (T-1)

2.6.5. Track, maintain, and analyze contractor security violations and infraction metrics and report them through Information Protection channels to SAF/AAZ when requested. Categorize these occurrences with the terms found in AFI 16-1404. (T-1)

2.6.5. **(AFMC)** AFI 16-1406, paragraph 2.6.5 only applies to security incidents caused by contractors working for integrated or NISPOM visitor groups. Send metrics through Center CIP to HQ AFMC/IP. HQ AFMC/IP will send the metrics to SAF/AAZ. **(T-2).**

2.6.6. Report adverse information and suspicious contact, security violations, and espionage, sabotage, and subversive activties in accordance with Chapter 5 of this AFI. (T-0)

2.6.7. Provide industrial security training for security managers as applicable.

2.6.8. Provide industrial security review data and derivative classification decisions for inclusion in Senior Agency Self-Inspection and Agency Security Classification Management Program Data reports. (T-0)

2.6.8. **(AFMC)** AFI 16-1406, paragraph 2.6.8 only applies to contractor integrated and NISPOM visitor groups. You would not collect this data at cleared contractor facilities for inclusion in an AF organizations Senior Agency Self-Inspection and Agency Security Classification Management Program Data reports.

2.6.9. Administer the DSS contractor reported security violations process and ensure a copy of the returned response is provided by program/project managers to SAF/AAZ. (T-0)

2.6.9. **(AFMC)** Copy of response will be sent through the Center CIP to HQ AFMC/IP. HQ AFMC/IP will send the response to SAF/AAZ. **(T-2).**

2.6.10. Process NID requests and provide guidance, as needed. (T-1) Process NID requests and responses through IP channels to SAF/AAZ. (T-1) SAF/AAZ will notify DSS, if applicable.

2.6.10. **(AFMC)** When a company requires a NID, the Contracting Officer with the assistance of the Program Manager and Security Manager will send a NID request to DSS; see **Attachment 2**. When access to AF TS information is required, DSS will need approval for collateral TS information from the OCA; see **Attachment 4** for a sample OCA TS NID request package. SAP NID requests will be processed through SAP channels. SCI NID requests will be processed through the supporting SSO to HQ AFMC/A2S. **(T-2).** Contact your servicing CIP for questions on collateral NID process. Contact HQ AFMC/A5/8Z, servicing GSSO, or PSO for questions on SAP NIDs. Contact the servicing SSO for questions on SCI NIDs. DSS NID office is Defense Security Service FOCI Operations Division, (571) 305-6306 or **nid@dss.mil.** DoD reference for NIDs see DoDM 5220.22, Volume 3 and DTM 15-002.

2.6.11. **(Added-AFMC)** Work closely with the host-installation Cybersecurity office (formerly information assurance). The host-installation Cybersecurity office will provide oversight to any approved contractor system/networks that process classified or controlled unclassified information to ensure those system/networks are properly accredited and all DoD/AF information technology cybersecurity requirements are met. **(T-2).**

2.6.12. **(Added-AFMC)** Maintain a folder (paper or electronic) on each visitor group for which a VGSA has been executed and for each cleared facility over which the installation commander retains security cognizance; see paragraph **6.5**. **(T-2).**

2.7. Contracting Officer Actions. In addition to requirements in this AFI, DoD 5220.22-R provides functional responsibilities within the industrial security program. As a minimum, contracting officers:

2.7.1. Notify the servicing Wing Information Protection Office:

2.7.1. **(AFMC)** The Center Information Protection Office may be the servicing IP office. For assistance in identifying servicing IP offices, contact your servicing IP office.

2.7.1.1. As soon as possible; no later than 30 days prior to contract award/modification.

2.7.1.1. **(AFMC)** CO notifies the servicing IP Office when a contract requiring performance on an Government installation and access to classified information is awarded or modified. For assistance in identifying which servicing IP office, contact your servicing IP office.

2.7.1.2. To request a NID when it is determined a company may have FOCI indicators and access to proscribed information. (T-0)

2.7.1.2. **(AFMC)** When a company requires a NID, the Contracting Officer with the assistance of the Program Manager and Security Manager will send a NID request to DSS; see **Attachment 2**. When access to AF TS information is required, DSS will need approval for collateral TS information from the OCA; see **Attachment 4** for a sample OCA TS NID request package. SAP NID requests will be processed through SAP channels. SCI NID requests will be processed through the supporting SSO to HQ AFMC/A2S. **(T-2).** Contact the servicing CIP for questions on collateral NID process. Contact HQ AFMC/A5/8Z, servicing GSSO, or PSO for questions on SAP NIDs. Contact the servicing SSO for questions on SCI NIDs. DSS NID office is Defense

Security Service FOCI Operations Division, (571) 305-6306 or **nid@dss.mil.** DoD reference for NIDs see DoDM 5220.22, Volume 3 and DTM 15-002.

2.7.2. Ensure DD form 254 is distributed in accordance with Chapter 3 of this AFI.(T-1)

2.7.3. Sign Block 16 of the DD Form 254 as the certifying official. (T-0)

2.8. System, Program, Project Managers, Commanders/Directors. These positions are referred to as program/project managers in this AFI**.** These positions are key to identification of specific types of information required by the contractor and security classification guidance by completing the DD Form 254. Program/project managers also play a critical role in identifying companies with access to proscribed information that may require a NID due to FOCI. In addition, program/project managers assist with the development of the VGSA, providing responses to security violations to DSS (and the Wing Information Protection office), and identifying and reporting changes that may affect a contracted company FCL.

2.8.1. Complete the DD Form 254 and identify the specific types of classified access needed to support contract performance and provide security classification guidance as needed. See Chapter 3 for specific guidance on completing the DD Form 254. (T-0)

2.8.2. Notify the servicing Wing Information Protection office 30 days prior to contractor work beginning (i.e., work or classified information access; a contract with a DD Form 254) and assist with development of the VGSA. (T-1)

2.8.2. **(AFMC)** Shall ensure unit notifications to servicing Wing IP offices protect contractor bid or proposal information and source selection information. **(T-2).** For assistance in

2.8.3. Process DSS reported security violation responses received from the servicing Wing Information Protection office to DSS and provide a copy to the wing. (T-0)

2.8.3. **(AFMC)** Security incident responses will be sent back through Center CIP. **(T-2).**

2.8.4. Changes that could affect the FCL i.e., indicators of FOCI. (T-0)

Chapter 3

THE DD FORM 254

3.1. Purpose. The DD Form 254 documents and communicates security requirements needed in performance of a classified contract. Program/project managers are responsible for completing the DD Form 254 for prime contracts. (T-1) The CO certifies the form in block 16. (T-0) The Defense Security Service website may be referenced for detailed guidance. The DD Form 254 can be located on the NISP Contract Classification System (NCCS) accessible on Wide Area Workflow (WAWF) at **https://wawf.eb.mil.**

3.1. (AFMC)Purpose. A DD Form 254 form will be included with the Request for Bid, Request for Proposal, Request for Information to clarify security requirements for the final contract award. When access to classified information is required during the acquisition process, a DD Form 254 shall be completed in the same manner as a DD Form 254 for awarding a

3.1.1. Ensure servicing Wing Information Protection office reviews and coordinates by annotating Block 13 with office symbol, date and initials of reviewer (T-0).

3.1.1. **(AFMC)** Servicing Center CIP may review and coordinate instead of the Wing IP office.

3.1.2. Submit DD Form 254 to the servicing contracting office for certification. (T-0)

3.1.2.1. Ensure contracts:

3.1.2.1.1. Incorporate language and appropriate contract clauses for protection of critical information identified in the Operations Security program IAW AFI 10-701, Chapter 8. (T-0)

3.1.2.1.2. Incorporate language and appropriate contracts clauses for the protection to classified information. (T-0)

3.1.2.1.3. Incorporate language and appropriate contract clauses for protection of unclassified controlled technical information IAW DFARS Subpart 204.73. (T-0)

3.1.2.1.3. **(AFMC)** Incorporate language and appropriate contract clauses for protection of covered defense information. **(T-2).**

3.2. Completing the DD Form 254. Complete all blocks on the DD Form 254. (T-0) The following blocks require special attention:

3.2.1. Block 3 This Specification Is: verify the intended specification for the DD 254. (T-0)

3.2.1.1. Original date refers to the release date of the DD Form 254. This date will not change and will be annotated on subsequent revisions of the DD Form 254. (T-0)

3.2.1.2. Revised DD Form 254s are issued when there is a change to classification guidance or security requirements of the contract.

3.2.1.3. ‘Final’ DD Form 254 is only used to authorize additional retention of classified materials beyond the terms of the contract.

3.2.2. Block 10 Contractor Will Require Access To: this block refers to access to various types of information required within the scope of the contract. If blocks 10a-f or TS access is

required, a notification for a NID request should flow through Information Protection channels to SAF/AAZ. See Chapter 5 for additional details.

3.2.2. **(AFMC)** See AFI 16-1406, paragraph 5.7 to determine when a NID is required. Formerly Restricted Data and non-Sensitive Compartmented Information are not categories of proscribed information. See AFI 16-1406, Atch 1, Terms for correct definition of proscribed information.

3.2.2.1. When program/project managers have identified information in Block 10 e (Intelligence Information; SCI) and access is necessary for contract performance on a DD Form 254, submit the NID Request with DD Form 254 to AF/A2 for processing.

3.2.2.2. If Block 10 f (Special Access Program; SAP) access is identified as necessary for contract performance on a DD Form 254, submit the NID Request to SAF/AAZ following the template in AFI 16-701.

3.2.3. Block 12 Public Release: Ensure "Through" block is marked and the following statement is included: Information requiring AF or DoD–level review will be forwarded by the entry-level public affairs office through the MAJCOM/DRU Public Affairs Office to the Secretary of the Air Force, Office of Public Affairs, Security and Review Division (SAF/PAX), 1690 Air Force Pentagon, Washington DC 20330-1690. (T-0)

3.2.4. Block 13 Security Guidance:

3.2.4.1. Be specific on security guidance.

3.2.4.2. Use this area to show coordination of security officials by annotating contact information and initials. (T-1)

3.2.4.3. Include program/project manager or designated representative by annotating name, office symbol, and contact information. (T-1)

3.2.4.3. **(AFMC)** Include unit security manager/specialist's name, office symbol and contact information. **(T-2).**

3.2.4.4. **(Added-AFMC)** The responsible Contracting Officer Representative or Program Manager will identify (by title, functional OPR, and approval date, to include letter changes), the specific security classification guidance or guides (SCG) applicable to the contract in block 13 of the DD Form 254. **(T-2).**

3.2.5. Block 16 Certification, is signed by the contracting office. (T-0)

3.2.6. Block 17 Required Distribution. If work is to be conducted at multiple locations or MAJCOMS, ensure the DD Form 254 is coordinated with those stakeholders. (T-1)

3.2.6. **(AFMC)** Coordination with stakeholders is done prior to submitting the DD Form 254 to the servicing CIP for coordination. Stakeholders are not required to annotate coordination on the DD Form 254. **(T-2).**

3.2.7. Provide the DD Form 254, justification for disclosure of classified information, and action officer or POC name and number. These are to be included on the DD Form 254. (T-1)

3.2.7. **(AFMC)** Properly filling out the DD Form 254 meets the requirement for justification of disclosing classified and the Program Manager information, required from AFI 16-1406,

paragraph 3.2.4.3, meets the requirement of the action officer or POC information. Forward AFRC stakeholder coordination to the AFRC/IP Workflow mailbox when contract performance is on an AFRC installation.

3.2.8. When DoD internal coordination is required for proscribed information at the Top Secret level e.g., AF-Navy-Army Top Secret, the NID request shall be processed (responded to) within 30 days. (T-1) Requests received from internal DoD partners require reply within 30 days. (T-1)

3.3. Distribution of DD Form 254. The CO will maintain a copy of the DD Form 254. (T-1) Distribution is made to:

3.3.1. Wing Information Protection Office for collateral information. (T-0)

3.3.1. **(AFMC)** Send the DD Form 254 to the servicing IP office when contractor performance is on an AF installation.

3.3.2. When SAP is involved, coordinate the DD Form 254 in accordance with AFI 16-701, Management, Administration and Oversight of Special Access Programs. Keep DD Forms 254 unclassified whenever possible. (T-0)

3.3.3. AF/A2 for SCI. Keep DD Forms 254 unclassified whenever possible. (T-0)

3.3.3. **(AFMC)** Send SCI DD Form 254 to the supporting SSO. **(T-2).**

3.3.4. DSS Headquarters, if DSS is relieved of security oversight responsibility. (T-0)

3.3.4. **(AFMC)** HQ Defense Security Service, 27130 Telegraph Rd, Quantico VA 22134.

Chapter 4

VISITOR GROUPS AND AGREEMENTS

4.1. General. Installation commanders categorize contractors operating on the installation as cleared facility, visitor groups, or intermittent visitors. (T-0) Cleared facilities are discussed in Chapter 5. Contractor operations performing less than 90 days qualify as intermittent visitors Intermittent visitors may operate under the security requirements of the NISPOM or the installation security program. Generally, contractor operations in excess of 90 days are designated visitor groups. Visitor Group limits and actions while on the installation are codified in Visitor Group Secuity Agreements.

4.2. Development of the VGSA. The industrial security specialist will ensure VGSA:

4.2.1. Incorporates the visitor group into the AF Information Security Program. (T-1)

4.2.2. A separate or independent VGSA is developed for subcontractors when prime and subcontractors are not working at the same AF installation. If at the same location, a separate VGSA is not required. (T-0)

4.2.2. **(AFMC)** When one VGSA is used for the prime and subcontractor, the subcontractor will acknowledge following the prime contractors VGSA; examples: sub signs VGSA, sub signs memo acknowledging to follow VGSA, prime includes VGSA requirement in sub's DD Form 254, etc. **(T-2).**

4.2.3. Prohibits Visitor Groups from establishing their own Information Technology (IT) systems/networks (Local Area Networks [LAN], Wide Area Network [WAN], Cellular phone/USB Modem as WAN, Wi-Fi as WAN, etc.) without the direct permission of governing communications and responsible information systems office. (T-0)

4.2.3. **(AFMC)** This requirement also pertains to NISPOM visitor groups. If permission is granted, the Government office approving the contractor system/network is responsible for providing oversight to the contractor's system/network to ensure the system/network is properly accredited and all DoD/AF information technology requirements are met. **(T-2).**

4.2.4. Require contractor employees who need access to government IT are determined to be trustworthy by a designated government official prior to IT access being granted. (T-0)

4.2.4. **(AFMC)** This is accomplished through the system authorization access request, DD Form 2875, process. See AFI 31-501 for background investigation requirements.

4.2.5. Use existing AF security program related plans (Operations Security, Program Protection, Information Technology, etc.), procedures, operating instructions, and educational/training materials that meet the intent of and satisfy NISPOM requirements. Coordinate with other security discipline OPRs, when applicable, and incorporate authority for their usage in the VGSA or other appropriate contracting documents. (T-0)

4.2.6. Is coordinated with the security discipline OPRs and DSS, if applicable. (T-1)

4.2.6. **(AFMC)** DSS is not required to coordinate on VGSAs.

4.2.7. Allows responsible security discipline OPR to accompany the industrial security specialist or CSO representative during security reviews or when requested. (T-0)

4.2.8. Subcontractors submit independent Visit Requests to the serviced organization via JPAS on their employees. (T-1)

4.2.8. **(AFMC)** Upon in-processing visitor group personnel, unit Security Managers will service the employee's record under their current employer category in JPAS to ensure immediate notification of a change in an individual's status or eligibility. The FSO will own the contractor in JPAS. Records will be unserviced upon the visitor group personnel out-processing the unit. Contractors will send visit request through their FSO not the sponsoring AF Security Managers unless specified in the contract. Security Managers will not change or add any items in JPAS for contractors. **(T-2).**

4.2.9. **(Added-AFMC)** Require integrated visitor groups to be part of the sponsoring AF organizations security education program, to include initial, recurring, and derivative classification security training. **(T-2).**

4.2.9.1. **(Added-AFMC)** Identify how NISPOM visitor groups will conduct required training. The contractors' facility security officer or NISPOM visitor group security point of contact will provide initial and recurring security training to NISPOM visitor group contractors. Recommend that NISPOM visitor group employees also be included in sponsoring AF organizations security training programs. **(T-2).**

4.2.10. **(Added-AFMC)** The installation commander, or CIP if designated, and an authorized representative of the contractor, normally the HOF FSO, will sign the VGSA. **(T-2).**

4.2.11. **(Added-AFMC)** The IP office forwards a copy of the signed VGSA to the Procuring Contracting Officer, AF sponsoring organization, and the contractors security focal point.

Chapter 5

REPORTING REQUIREMENTS

5.1. Clearances. There are two types of clearances within the industrial security program. A Facility Security Clearance (FCL) is an administrative determination by Defense Security Service (DSS) that a company is eligible for access to classified information. The other clearance is Personnel Security Clearance (PCL)**.** A PCL is an administrative determination that a contractor is eligible for access to classified information. The FCL can be affected if adverse information results in the removal of a PCL, or change introducing FOCI indicators of those identified as key management personnel.

5.2. Requesting a FCL. Most companies bidding on a classified contract have an FCL. However, a company may be awarded a contract and not be in possession of an FCL. Should this occur, the contracting office initiate a request for an FCL. (T-0) A sample FCL request letter can be obtained from the Defense Security Service (DSS) website, Industrial Security page.

5.2.1. A company's FCL can be verified through the Industrial Security Facilities Database (ISFD) maintained by DSS.

5.2.1. **(AFMC)** ISFD can verify the company's safeguarding capability, address, CAGE code, and if the company requires a NID for access to proscribed information.

5.2.1.1. To gain access to the ISFD complete the ISFD System Access Request form located on the DSS website, Information Systems ISFD web page.

5.2.1.2. This information is used to complete Block 1 of the DD Form 254.5.2.2. It is U.S. policy to support foreign investment in the United States consistent with the protection of the national security. Foreign Ownership, Control, or Influence (FOCI) is a set of processes which may facilitate foreign investment in the US. These processes become necessary to make a determination that access to national defense information by companies impacted by FOCI is considered. DSS processes FOCI actions and any subsequest NID when needed. SAP NID questions/submissions will be reported to the MAJCOM SAP Management Office.

5.2.2. **(Added-AFMC)** When a company requires a NID, the Contracting Officer with the assistance of the Program Manager and Security Manager will send a NID request to DSS; see **Attachment 2**. When access to AF TS information is required, DSS will need approval for collateral TS information from the OCA; see **Attachment 4** for a sample OCA TS NID request package. SAP NID requests will be processed through SAP channels. SCI NID requests will be processed through the supporting SSO to HQ AFMC/A2S. **(T-2).** Contact your servicing CIP for questions on collateral NID process. Contact HQ AFMC/A5/8Z, servicing GSSO, or PSO for questions on SAP NIDs. Contact the servicing SSO for questions on SCI NIDs. DSS NID office is Defense Security Service FOCI Operations Division, (571) 305-6306 or **nid@dss.mil.** DoD reference for NIDs see DoDM 5220.22, Volume 3 and DTM 15-002.

5.2.2.1. Program/project manager, contracting office, becoming aware of the sale of a contract or a company subject to FOCI must report this information to the servicing Wing Information Protection Office. (T-1)

5.2.2.2. Information Protection offices will relay this information to SAF/AAZ through IP channels. (T-1)

5.2.2.2. **(AFMC)** Center CIP will relay this information to SAF/AAZ through HQ AFMC/IP. **(T-2).**

5.3. Reporting Adverse Information and Suspicious Contacts. Actions or behaviors which may cause question of an employees trustworthiness, reliability, or judgment concerning their access to classified information are considered Adverse Information. Personnel working with or near classified information are possible targets of persons our contry's adversaries or even those with a casual interest in national defense. Reporting suspicious contacts assist in safeguarding critical defense information. Visitor Groups and cleared facilities report these occurrences to the Information Protection office. This reporting requirement will be specified in the VGSA. (T-0)

5.3.1. Visitor Groups report occurences to Information Protection office through their unit. (T-1)

5.3.2. Cleared facilities report occurences to the Wing Information Protection Office. (T-1)

5.3.3. The Wing Information Protection Office will:

5.3.3.1. Notify other AF activities, e.g., contracting office, Air Force Office of Special Investigations (AFOSI), when appropriate. (T-1)

5.3.3.2. Report information to the visitor group's Home Office Facility (HOF). (T-1)

5.3.3.2. **(AFMC)** Send report through the Contracting Officer. **(T-2).**

5.3.3.3. The servicing Wing Information Protection Office will retain a copy of any adverse information or suspicious contact reports in accordance with Air Force Records Management standards. (T-1)

5.3.3.4. HOF performs any subsequent or additional reporting required by the NISPOM.

5.4. Reporting Security Violations.

5.4.1. Refer to AFI 16-1404 for inquiry/investigation/reporting requirements occurring on an installation. Visitor groups report violations through their unit to the Wing Information Protection Office. (T-1) Cleared facilities report directly to the Wing Information Protection Office. The Wing Information Protection Office report security violations to HOF for cleared facilities. (T-1)

5.4.1. **(AFMC)** When contractors cause security incidents on AF installations, notify the contractor's FSO and Contracting Officer. **(T-2).**

5.4.2. Program/project managers will respond to the DSS requirements and provide the Wing Information Protection Office a copy of the response. (T-0)

5.4.2. **(AFMC)** Security incident responses will be sent back through Center CIP. **(T-2).** Original Classification Authorities are responsible for conducting damage assessments. See DoDM 5200.01, Vol 3, Enclosure 6.

5.4.2.1. These are cases of external Security Violation processing. The AF receives notice of security violations occurring at an industry concerning information an AF

program or project manager uses is at risk or has been compromised. Specifc instructions are provided for each occurrence.

5.5. Reporting Espionage, Sabotage, and Subversive Activities. Suspicious activities may extend beyond the AF and endanger the defense industrial framework of our nation and its governing principles. When this occurs external government investigative agencies may need to be notified.

5.5.1. To expedite notifications, Visitor Groups and cleared facilities report these incidents directly to both the Wing Information Protection Office and AFOSI. The report should identify:

5.5.1.1. The Visitor Group or cleared facility.

5.5.1.2. All person(s) involved to include full name, date and place of birth, social security number, local address, present location, position within the company, and security clearance. Adhere to Personal Identity Information guidelines.

5.5.1.3. Any past or present participation in special access programs (SAPs).

5.5.1.4. Facts of the incident (who, what, when, where, why, and how).

5.5.1.5. Level of classified information involved and description (document, material, equipment, etc.,).

5.5.1.6. Whether news media know about the incident and if so which one(s).

5.5.1.7. Culpable individuals, if known.

5.5.1.8. Changes in contractor procedures necessitated by the incident and any recommendations for change in the security program, which may prevent similar violations.

5.5.2. Protect and mark reports containing personal identifiable information or any other exemption under the Freedom of Information Act (FOIA) as For Official Use Only (FOUO) in accordance with DoD 5200.01-M, Volume 4. (T-0)

5.5.3. The Wing Information Protection Office will ensure that the MAJCOM/DRU is notified. Include the servicing Public Affairs for incidents of information released to the media. (T-1)

5.5.3.1. Include a copy of any reports. (T-1)

5.5.3.2. Describe of any plans or action to safeguard and any recommendations to suspend or revoke an individual’s personnel security clearance (PCL). (T-1)

5.5.4. AFOSI notifies external investigative agencies as required.

5.6. Invalidation of FCL. Invalidation of FCL renders a contractor ineligible to bid on new classified contracts or receive new classified material. If a Visitor Group or cleared facility loses their FCL the Wing Information Protection Office:

5.6.1. Notify SAF/AAZ through Information Protection channels. (T-0)

5.6.1. **(AFMC)** Center CIP notifies SAF/AAZ through HQ AFMC/IP. **(T-2).**

5.6.2. Instruct the contractor to return the classified material in its possession, unless otherwise directed. (T-0)

5.6.2. **(AFMC)** CIPs shall coordinate with the Contracting Officer, Contracting Officer's Representative, affected unit and other security disciplines, as applicable, for return of classified information. **(T-2).**

5.7. Reporting FOCI and NID Requests. A company may encounter growth or other situations which present foreign ownership, control, or influence (FOCI) indicators. While not exclusive to program/project managers, they are in a position to observe and learn of information and conditions that may surface FOCI and play a critical reporting role that may result in a NID.

5.7. (AFMC)Reporting FOCI and NID Request. A NID is required when a cleared company has FOCI, operates under an approved Special Security Agreement (SSA) from DSS, and requires access to proscribed information. See AFI 16-1406, Atch 1, Terms, for definition of proscribed information. See DoDM 5220.22, Volume 3, National Industrial Security Program: Procedures for Government Activities Relating to Foreign Ownership, Control or Influence (FOCI) and DTM 15-002, Policy Guidance for the Processing of National Interest Determinations in Connection with FOCI.

5.7.1. NID requirements:

5.7.1.1. Confirm release of proscribed information to the U.S. contractor is consistent with the national security interest of the United States (requires a documented justification). Identify proscribed information:

5.7.1.1.1. Blocks 10 a, e, or f of the DD Form 254 are annotated. (T-0)

5.7.1.1.1. **(AFMC)** Blocks 10 a, b, c, e(1), or f. See Attachment 1, Terms, for the correct definition of proscribed information.

5.7.1.1.2. Top Secret access is required in the performance of the contract or any of the contract's supporting documentation. (T-0)

5.7.1.2. Identify the FOCI condition(s). FOCI applies if the company is:

5.7.1.2.1. In pre-contract activities. (T-0)

5.7.1.2.2. Already cleared under a special security agreement (SSA) and the work to be performed is a new contract. (T-0)

5.7.1.2.2.1. If unable to determine if a company is cleared under a SSA make the notification. (T-0)

5.7.1.2.2.1. **(AFMC)** To determine if company is cleared under a SSA, call DSS or look the company up in DSS's ISFD. See DoDM 5220.22, Volume 3.

5.7.1.2.3. In the process of obtaining a facility security clearance (FCL). (T-0)5.7.1.2.4. Acquired by foreign interests or a change in Key Management Personnel (KMP) that provide indicators of foreign ownership, control or influence. (T-0)

5.7.1.3. Notify the Wing Information Protection Office which processes the NID notification to SAF/AAZ. (T-1) Refer SAP NID questions/submissions to the appropriate MAJCOM SAP Management Office. (T-0)

5.7.1.3. **(AFMC)** When a company requires a NID, the Contracting Officer with the assistance of the Program Manager and Security Manager will send a NID request to DSS; see Attachment 2. When access to AF TS information is required, DSS will need approval for collateral TS information from the OCA; see **Attachment 4** for a sample OCA TS NID request package. SAP NID requests will be processed through SAP channels. SCI NID requests will be processed through the supporting SSO to HQ AFMC/A2S. **(T-2).** Contact your servicing CIP for questions on collateral NID process. Contact HQ AFMC/A5/8Z, servicing GSSO, or PSO for questions on SAP NIDs. Contact the servicing SSO for questions on SCI NIDs. DSS NID office is Defense Security Service FOCI Operations Division, (571) 305-6306 or **nid@dss.mil.** DoD reference for NIDs see DoDM 5220.22, Volume 3 and DTM 15-002.

Chapter 6

OVERSIGHT REVIEWS

6.1. Conducting Security Reviews (SRs) at Cleared Facilities: (NOTE: As used in this publication the term "security review" is not synonymous with nor does it negate the "security and policy review" requirement of AFI 35-101, *Air Force Public Affairs Policies and Procedures*.)

6.1.1. The Wing Industrial Security Specialist conducts security reviews of cleared facilities that perform classified work on AF installations when the Installation Commander retains oversight responsibilities. (T-1)

6.1.1. **(AFMC)** CIPs conduct security reviews of cleared facilities, for which they maintain security oversight, at least annually. **(T-2).**

6.1.2. Scheduling Security Review. Provide contractor activity management 30 days advanced written notification. (T-0)

6.1.3. Performing Security Review. Industrial security specialist coordinate with other AF security discipline OPRs; Operations Security (OPSEC), Computer Security (COMPUSEC), and Communications Security (COMSEC), etc., to provide specialized expertise when necessary to complete a security review. (T-0) The security review is complete when all security requirements imposed under the terms of the contract have been evaluated.

6.1.3. **(AFMC)** The servicing host-installation Cybersecurity (formerly information assurance) official will participate in security reviews of cleared facilities when the cleared facility has systems/networks that process classified or controlled unclassified information. **(T-2).**

6.1.4. Post-Security Review Requirements.

6.1.4.1. Send a letter/report to senior management officials of the cleared facility within 10 days of completing the security review. The letter will:

6.1.4.2. Confirm the assessment of the contractor security program as discussed during the exit interview. (T-0)

6.1.4.3. List any deficiencies requiring corrective action. (T-0)

6.1.4.4. , Request written confirmation be provided within 30 days of the deficiencies, remedy, and status of any open major discrepancy (condition which resulted in or could reasonably be expected to result in the loss or compromise of classified information). (T-0)

6.1.5. Unsatisfactory Security Review.

6.1.5.1. The industrial security specialist assigns a cleared facility an unsatisfactory security review rating:

6.1.5.1.1. If the cleared facility fails to satisfactorily perform contractual security responsibilities. (T-0)

6.1.5.1.2. When major failures in the contractor security program have resulted in or could reasonably be expected to result in loss or compromise of classified information. (T-0)

6.1.5.1.3. When the contractor is clearly responsible for the security problems cited during a security review. (T-0)

6.1.5.2. The industrial security specialist coordinates with the contracting officer when assigning an unsatisfactory security review rating for a cleared facility. (T-0)

6.1.5.3. The HOF for the cleared facility is ultimately responsible for meeting contract security requirements.

6.1.5.3.1. When assigning an unsatisfactory security review rating, the industrial security specialist notifies the HOF immediately through the contracting office and requests prompt and complete corrective action.

6.1.5.3.2. Industrial security specialists notify HOF if problems continue. (T-1)

6.2. Self-Inspections and Self-assessments for Visitor Groups. Wings and sponsoring AF activities will include contractor visitor groups within their self-inspection and self-assessment programs; see AFI 16-1404. (T-1)

6.2. (AFMC)Self-Inspections and Self-assessment for Visitor Groups. The CIP will conduct industrial security reviews of NISPOM visitor groups IAW the NISPOM and VGSAs at least annually. The CIP will conduct these reviews separately from host unit security self-inspections explained in AFI 16-1404. NISPOM visitor groups will conduct self-inspections of their security programs in accordance with the NISPOM. Integrated visitor groups will be included in the host units inspection explained in AFI 16-1404 and the host units self-assessment explained in AFI 90-201. **(T-2).**

6.3. Security Discipline Assessment/Inspection Reciprocity. The CO, industrial security specialist, and other Wing (or installation security discipline offices) of primary responsibility (OPRs) work together to resolve issues pertaining to reciprocity, as applicable to assessments, surveys, audits, security clearances, security reviews, etc.

6.4. Contract Closeout or Termination. The program office, requiring AF activity or CO will notify the Wing industrial security specialist in writing when the contract performance has been completed or terminated in order to schedule a close-out inspection. (T-0)

6.4. (AFMC)Contract Closeout or Termination. Ensure all classified information has been returned to the Government or destroyed. See DoD 5220.22-R, paragraph C4.3 for more information on close-out inspections.

6.5. (Added-AFMC) Contractor Folder. The CIP, unit security manager, and visitor group (or cleared facility) establishes files and maintains the following documentation, as appropriate: **(T-2).**

6.5.1. **(Added-AFMC)** Signed copy of the DD Form 254 and any revisions; prime and subcontractor. **(T-2).**

6.5.2. **(Added-AFMC)** Signed copy of the VGSA. For subcontracts, either a separate VGSA or something showing the subcontractor will follow the prime contractors VGSA. Not needed for a cleared facility. **(T-2).**

6.5.3. **(Added-AFMC)** Signed copy of consultant agreements. **(T-2).**

6.5.4. **(Added-AFMC)** Copy of the last annual program review/inspection; prime and subcontractor as applicable. **(T-2).**

6.5.4.1. **(Added-AFMC)** Cleared facilities and NISPOM visitor groups receive and maintain copies of their last CIP industrial security review reports. **(T-2).**

6.5.4.2. **(Added-AFMC)** Integrated visitor groups are included in CIP security self-inspections of their host activities explained in AFI 16-1404. These groups receive and maintain copies of information pertaining to their groups from their host government activities' inspection reports. They do not receive or maintain the entire report. **(T-2).**

6.5.5. **(Added-AFMC)** Copies of last self-assessment; prime and subcontractor as applicable. (***NOTE:*** The maintenance of self-assessments is optional for CIPs). **(T-2).**

6.5.5.1. **(Added-AFMC)** Unit security managers maintain copies of the host activities' self-assessments. Integrated visitor groups maintain portions of self-assessment reports applicable to their operation. **(T-2).**

6.5.5.2. **(Added-AFMC)** Cleared facilities maintain copies of their self-inspections conducted in accordance with the NISPOM. **(T-2).**

Chapter 7

VISITS AND MEETINGS

7.1. Installation Visitors. The installation commander is the authority responsible for granting contractors access to the installation, regardless of which DoD agency, military service component, or activity awarded the contract.

7.1. (AFMC)Installation Visitors. See AFMAN 31-113, *Installation Perimeter Access Control*, for guidance regarding access to an installation.

7.2. Contractor Visits to AF Installations. DoD contractors located on or visiting AF installations in support of a classified contract must comply with DoD 5220.22-M, Chapter 6, Section 1, visit requirements. (T-0) Joint Personnel Adjudication System (JPAS) is the system of record for confirming classified access eligibility for DoD employees and all contractor personnel. (T-0)

7.2. (AFMC)Contractor Visits to AF Installations. Security managers will service integrated and NISPOM visitor group contractors (prime and sub) within JPAS. Contractors will send visit request through their FSO not the sponsoring AF organization, unless specified in contract. **(T-2).** Also see paragraph **4.2.8**.

7.2.1. **(Added-AFMC)** Prior to granting contractors access to classified information, in addition to AFI 16-1404, para 5.1.1.1.1 thru 5.1.1.1.3, verify the information/accesses are authorized via the DD Form 254 on the contract. In the case of a subcontractor, review the subcontract DD Form 254. **(T-2).**

7.3. AF Visits to Contractor Facilities. AF personnel who require access to classified information while visiting commercial contractor facilities must comply with the visit request submission requirements of DoD 5200.01-M V1-4 and AFI 16-1404, DoD 5220.22-M, and/or the contractor location to be visited. (T-0).

Chapter 8

SPECIAL REQUIREMENTS

8.1. Special Access Program. The AF assumes cognizance (instead of DSS for oversight responsiblity) of Special Access Program contracts. Program Security Officers (PSO) coordinate with the appropriate contracting officer (CO) and program manager (PM) to validate DD Forms 254 contain language indicating DSS is "carved out" of program oversight and identifies AF Office of Special Investigations, Office of Special Projects (AFOSI/PJ) as having security and compliance inspection responsibility in accordance with the NISP and AF authorities (T-0). In these cases, a DD Form 254 may be completed only after endorsement by a PM and PSO. (T-0) COs may not delegate the authority to approve a SAP DD 254 (for specific SAP guidance also see DoD 5220.22M-Sup 1, NISPOM Supplement, NISP, AFPD 16-7 and AFI 16-701, *Special Access Programs)*. Non-SAP classified material and CUI kept within a SAPF does not fall within the assessment (or self-assessment) purview of the industrial security specialist. Responsibility for such material rests with the applicable PSO. (T-0)

8.1. (AFMC)Special Access Program. This does not alleviate coordination with the servicing IP Office. Program manager shall coordinate the DD Form 254 with the servicing IP Office and other security disciplines as applicable. **(T-2).**

8.2. Sensitive Compartmented Information. Program managers for SCI may relieve DSS and AF from security review and oversight responsibility for cleared facilities and/or visitor groups. This relief is normally limited to specific SCI information. Non-SCI classified material and CUI kept within a SCIF does not fall within the assessment purview of the Information Protection office. Responsibility for such material rests with the applicable SSO.

8.2. (AFMC)Sensitive Compartmented Information. This does not alleviate coordination with the servicing IP Office. Program Manager shall coordinate the DD Form 254 with the servicing IP Office and other security disciplines as applicable. **(T-2).**

8.3. Other Access Considerations. The CO will engage program managers to validate a DD Form 254 requires access and adherence to other programs (e.g., Personnel Reliability Program (PRP), Restricted Data (RD), Critical Nuclear Weapons Design Information (CNWDI), Nuclear Command and Control Extremely Sensitive Information (NC2 ESI) and NATO. (T-0)

8.4. NATO. AF organizations will:

8.4.1. Ensure contracts requiring access to NATO classified materials is included on a DD Form 254 when applicable. (T-0) A NATO briefing will be completed prior to granting access to the Secure Internet Protocol Router Network (SIPRNet). Refer to AFI 16-1404 for granting personnel access to NATO information. (T-1)

8.4.1.1. Integrate their visitor group contractors into the servicing NATO control point security program. (T-0)

8.4.1.2. If NATO approved computer network or standalone system access is required, annotate the need on the DD Form 254. (T-0)

8.4.1.3. Ensure NATO access for employees are approved by the contractor company, to include providing initial briefings and debriefings. (T-0) This should be clearly stated in either the contract Statement of Work (SOW), DD Form 254, or VGSA.

8.4.1.3. **(AFMC)** Include in the Performance Work Statement (PWS), DD Form 254, or VGSA that the company will update JPAS with NATO access. **(T-2).**

8.4.1.4. Instructions and responsibilities for the protection of NATO material will be clearly stated in the DD Form 254 or VGSA. (T-0)

8.5. Controlled Unclassified Information (CUI):

8.5.1. Ensure local policies for awarding contracts and VGSA, include the requirement for security training and education in all contracts that require or will have access to classified or CUI. (T-0) See DoD 5200.1-M, Volume 4.

8.5.2. CUI will be marked in accordance with DoD 5200.1-M, Volume 4. (T-0)

8.5.3. NATO and material identified as foreign government information are not CUI.

Chapter 9

INTERNATIONAL SECURITY REQUIREMENTS

9.1. Categorizing Contractor Operations Overseas. DoD policy does not allow an FCL to be issued for contractors located outside the US, Puerto Rico, or a US possession or trust territory. Treat DoD contractor operations supporting the AF overseas as visitor groups.

9.2. Disclosure of Information to Foreign Visitors/Interests. Visits by foreigners to contractors performing on AF contracts (whether on or off base) which require access to classified or controlled unclassified information will be processed according to AFI 16-201, AF Foreign Disclosure and Technology Transfer Program. (T-1) Requests to disclose classified, controlled unclassified, and other types of information must be coordinated and approved by the servicing AF foreign disclosure office with the appropriate delegated disclosure authority. (T-1) Refer to AFI 16-201 for further information.

9.2. (AFMC)Disclosure of Information to Foreign Visitors/Interests. AFLCMC/WFNJ is AFMC's Foreign Disclosure Office.

9.3. Documentary Disclosure of Information to a Foreign Entity. Contractors performing on AF contracts will submit requests for disclosure of classified or controlled unclassified information to the contracting officer. (T-1) The contracting officer will validate the need for disclosure and forward the request for information to the servicing AF foreign disclosure office with appropriate delegated disclosure authority. (T-0) The servicing AF foreign disclosure office will process the request in accordance with AFI 16-201. (T-1)

9.4. Foreign Visits. All visit requests to Visitor Groups or a Cleared Facility submitted by or on behalf of a foreign government must be processed through the installation and/or MAJCOM or DRU foreign disclosure activity, at least 30 days in advance of the intended arrival date. (T-1)

9.5. (Added-AFMC) Contract or Letter of Agreement. The contract or Letter of Offer and Acceptance that requires transfer of classified material to a foreign government at a point within the U.S., its territories, or possessions must designate a point of delivery and include a transportation plan or requirement to prepare a transportation plan. **(T-2).**

9.5.1. **(Added-AFMC)** CIPs must be involved with responsible program offices early in the planning stages in establishing special protection requirements for contracts with performance on foreign government installations that require contractors to access and maintain classified that is not releasable to the customer country government. The plan must include US Government employee involvement. Storage, custody, and control of classified information required by a US contractor employee abroad are the responsibility of the US Government. Therefore, the storage of classified information by contractor employees at any location abroad that is not under US Government control is prohibited. See DoDM 5200.1, Volume 3 and DoD 5220.22-M. **(T-2).**

9.5.2. **(Added-AFMC)** The foreign government involved in a Foreign Military Sales (FMS) contract normally assumes industrial security oversight and control of contractors supporting FMS requirements on their installation when the US classified information is releasable to the foreign government. They impose their own industrial security program on the classified

contract unless there is a requirement for contractor access to classified information that is not releasable to the foreign country. **(T-2).**

9.5.2.1. **(Added-AFMC)** If the information is not releasable to the foreign government, US Government employees must be involved. The storage of classified information by contractor employees at any location abroad that is not under US Government control is prohibited. **(T-2).**

9.5.2.2. **(Added-AFMC)** Letter of Offer and Acceptance needs to include the foreign government is required to provide security protection to US classified material released under the agreement that is at least equal to that afforded it by the US Government. If non-releasable US information will be involved, also include that an area will be provided for exclusively use by US personnel. See DoDM 5200.01, Volume 3, Enclosure 3, Paragraph 5. **(T-2).**

9.5.2.3. **(Added-AFMC)** If FMS contract support is on a US Government installation, the appropriate DoD or US military authorities provide security oversight and support. **(T-2).**

PATRICIA J. ZARODKIEWICZ
Administrative Assistant

(AFMC)

DAVID D. DAY, GS-15, DAF
Director of Information Protection

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

AFI 33-360, *Publications and Forms Management*, 25 September 2014

AFPD 16-14, *Security Enterprise Governance,* July 24, 2014

DoD 5220.22-M, *National Industrial Security Program Operating Manual (NISPOM),* February 28, 2006

DoD 5220.22-R, *Industrial Security Regulation,* December 4, 1985

DoDM 5220.22-V3, *National Industrial Security Program: Procedures for Government Activities Relating to Foreign Ownership, Control, or Influence (FOCI)*: 17 Apr 14

DoDM 5200.01-V1, *DoD Information Security Program,* February 24, 2012

DoDM 5200.01-V2, *DoD Information Security Program,* February 24, 2012

DoDM 5200.01-V3, *DoD Information Security Program,* February 24, 2012

DoD Manual 5200.01-V4, *DoD Information Security Program,* February 24, 2012

United States Security Authority for NATO Affairs (USSAN) 1-07, April 5, 2007

DFARS clause 252.204-7012, Safeguarding of Unclassified Controlled Technical Information, December 16, 2014

AFMAN 33-363, *Management of Records,* March 1, 2008

AFI 31-401, *Information Security Program Management,* November 1, 2005

AFI 16-1404, *The Air Force Information Security Program,* 29 May 2015

AFI 35-101, *Air Force Public Affairs Policies and Procedures,* August 18, 2010

Subpart 204.404-70, *Defense Federal Acquisition Regulation Supplement* (DFARS),

August 17, 1998 as amended

DoD 5200.2-R, Personnel Security Program, December 6, 1986

Federal Acquisition Regulation Part 4, 4.1303, 52.204-9 Personal Identity Verification of Contractor Personnel, OMB Guidance M-05-24, August 5, 2005

AFI 33-115, *Air Force Information Technology (IT) Service Management*, September 16, 2014

The Joint Air Force - Army - Navy (JAFAN) 6/0, Special Access Program Security Manual,

Revision 1, 29 May 2008

AFI 16-201, *Air Force Foreign Disclosure and Technology Transfer Program,* July 23, 2014

AFMAN 31-113, *Installation Perimeter Access Control*, 2 February 2015

Prescribed Forms

None

Adopted Forms

AF Form 847, *Recommendation for Change of Publication*

DD Form 254, Department of Defense Contract Security Classification Specification

Abbreviations and Acronyms

ACO—Administrative Contracting Officer

AFI—Air Force Instruction

AFOSI—Air Force Office of Special Investigations

AFPD—Air Force Policy Directive

AIS—Automated Information System

CO—Contracting Office

COMSEC—Communications Security (COMSEC)

CSO—Cognizant Security Office

CUI—Controlled Unclassified Information

DOD—Department of Defense

DOE—Department of Energy

DRU—Direct Reporting Unit

DSS—Defense Security Service

FAR—Federal Acquisition Regulation

FBI—Federal Bureau of Investigations

FCL—Facility Security Clearance

FOA—Field Operating Agency

FOCI—Foreign Ownership, Control, or Influence

HOF—Home Office Facility

IT—Information Technology

JPAS—Joint Personnel Adjudication System

ISS—Industrial Security Specialist

NID—National Interest Determination

NISPOM—National Industrial Security Program Operating Manual

OPR—Office of Primary Responsibility

OPSEC—Operations Security

PCL—Personnel Security Clearance

PCO—Procuring Contracting Officer

PSO—Program Security Officer

PM—Program Manager

SAF—Secretary of the Air Force

SAP—Special Access Program

SAV—Staff Assistance Visit

SCI—Sensitive Compartmented Information

SOO—Statement of Objectives

SOW—Statement of Work

VGSA—Visitor Group Security Agreement

Terms

Classified Contract—Any contract that requires or will require access to classified information by the contractor or the employees in the performance of the contract. A contract may be classified even though the contract document itself is not classified.

Cleared Facility—A non-government owned and operated industrial, educational, commercial, or other facility for which DoD has made an administrative determination (from a security viewpoint) that the entity is eligible for and requires access to classified information of a certain category (Confidential, Secret, or Top Secret).

Cognizant Security Agency (CSA).—Executive Branch Agencies authorized to establish an industrial security program to safeguard classified information under the jurisdiction of those agencies when disclosed or released to U.S. Industry. These agencies are DoD, DHS, DOE, CIA, and NRC.

Cognizant Security Office—The designated Department of Defense (DoD) agency responsible for industrial security program administration. The Secretary of Defense (SedDef) has designated the Defense Security Service (DSS) to perform this function. The DSS Director has further delegated this responsibility downward within the agency. DSS Regional Directors provide industrial security administration for contractor facilities located within their respective geographic area. One exception for which AF has responsibility is DoD contractors on AF installations designated as "visitor groups."

Functional Office of Primary Responsibility (OPR)—Functional OPR examples are a SAF directorate, A-Staff, or squadron that manages a security discipline and its associated proscribed or collateral information/material/equipment. Examples are A/2 or local SSO office for SCI; SAF-CIO, A/6, or communications squadron for COMSEC; etc.

Industrial Security—the element of the security enterprise to ensure the safeguarding of

classified information when in the possession of U.S. industrial organizations, educational institutions, and organizations or facilities used by contractors.

Industrial Security Specialist—This AF position administers the industrial security program most commonly located on a Wing staff at an installation. The industrial Security Specialist is responsible for overseeing contractor security programs and/or operations through an executed (signed by both parties) VGSA.

Installation—An installation is an area in which the AF holds a real property interest or real property over which the AF has jurisdiction by agreement with a state or foreign government or by right of occupation. The term installation also includes all off-base or detached installations under the jurisdiction of the commander of the primary installation.

Intermittent Visitor—A contractor or company, cleared per the National Industrial Secutiy Program (NISP) or Industrial Security Regulation, that require "entry" to an AF installation for brief periods of time on a scheduled or on call basis to perform contractual duties. An intermittent visitor's presence on an installation does not usually exceed 90 consecutive days.

Invalidation—A condition at a cleared facility caused by changed conditions or performance under which the facility may no longer be eligible for an FCL unless the facility promptly initiates appropriate corrective actions.

Major Discrepancy—A condition, which resulted in or could reasonably be expected to result in the loss or compromise of classified information.

National Industrial Security Program Operating Manual (NISPOM)—DoD 5220.22-M establishes the standard procedures and requirements for all government contractors, with regards to classified information.

National Interest Determination—a determination that contractor access to proscribed information is consistent with the national security interests of the United States.

Proscribed Information—Proscribed information is Top Secret (TS); Communications Security (COMSEC) material, excluding controlled cryptographic items when unkeyed and utilized with unclassified keys; Restricted Data (RD); Special Access Program (SAP); and sensitive compartmented information (SCI).

Reciprocity—A reciprocal condition, relationship, mutual or cooperative agreement, between two or more agencies, components, or departments agreeing to recognize and accept the efforts (e.g., requirements, procedures, actions, etc.) of the other in exchange for the same reparation.

Visitor Group—Any contractor operation, cleared per the NISP or Industrial Security Regulation that requires access to classified information (excluding a cleared facility). A contractor on an installation less than 90 days is categorized as an Intermittent Visitor and does not rquire a VGSA. The Installation Commander determines the categorization of the contractor operation based on the interaction with the serviced unit.

Visitor Group Security Agreement— The VGSA is installation and Wing specific and traces its existence to installation commander authority for allowing personnel to access a military installation; a documented and legally binding contractual agreement between an AF and a DoD contractor whereby the contractor commits to complying with, rendering, or performing specific security tasks or functions for compensation. The VGSA is different from, and in addition to the DD Form 441, **Department of Defense Security Agreement**, and DD Form 254, **DoD Contract Security Classification Specifications,** which are required.

Attachment 1 (AFMC)

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

Directive-type Memorandum (DTM) 15-002, *Policy Guidance for the Processing of National Interest Determinations in Connection with FOCI*, 11 February 2015

AFI 25-201, *Intra-Service, Intra-Agency, and Inter-Agency Support Agreements Procedures*, 18 October 2013

AFI 90-201, *The Air Force Inspection System*, 2 August, 2013

Prescribed Forms

None

Adopted Forms

None

Abbreviations and Acronyms

AEDC – Arnold Engineering Development Complex

CIP – Chief, Information Protection

GCA – Government Contracting Activity

GSSO – Government SAP Security Officer

GSU – Geographically Separated Unit (GSU)

IP – Information Protection

MOU – Memorandum of Understanding

MOA – Memorandum of Agreement

OCA – Original Classification Authority

PEO – Program Executive Officer

PWS – Performance Work Statement

SCG – Security Classification Guide

SSA – Special Security Agreement

SSO – Special Security Officer

TS – Top Secret

Terms

NISPOM Visitor Group—A contractor operation performed on an AF installation that does not meet the requirements of a cleared facility or integrated visitor group. A NISPOM visitor group operates in accordance with the NISPOM, VGSA, and installation security program requirements. They handle, generate, process, and store classified information separately IAW

their contracts and guidance provided in the VGSA. The visitor group has access to a security container or containers under the visitor group's control. Their access is limited to need-to-know contract-specific classified information. The CIP conducts industrial security reviews in accordance with the NISPOM, VGSA, and installation security program requirements.

Attachment 2 (Added-AFMC)

NATIONAL INTEREST DETERMINATION (NID) PROCESS

A2.1. (AFMC) Special Access Program (SAP): SAP NIDs are processed through SAP channels. Program Managers and Contracting Officers will contact HQ AFMC/A5/8Z, servicing Government SAP Security Officer (GSSO), or Program Security Officer (PSO) for questions on how to process SAP NIDs. SAF/AAZ approves SAP NIDs; SAF/AAZ sends approved NIDs to DSS for them to update their database.

A2.2. (AFMC) Sensitive Compartmented Information (SCI): Program Managers and Contracting Officers will contact their servicing Special Security Officer (SSO) for questions on how to process SCI NIDs. SCI NIDs are approved by Office of Director of National Intelligence (ODNI).

A2.3. (AFMC) Communications Security (COMSEC) material, excluding controlled cryptographic items when unkeyed and utilized with unclassified keys: Program Manager creates NID request memo; Program Executive Office (PEO) signs memo; Contracting Officer sends memo to DSS; DSS sends memo to NSA for approval. Contracting Officer with help from the servicing IP Office sends a copy of the approved NID to SAF/AAZ.

A2.3.1. **(AFMC)** DSS requires a formal signed memorandum addressed to NSA requesting COMSEC access. The memo must contain a detailed COMSEC list as well as the reason/justification why access to COMSEC is necessary. DSS will forward this memo, along with all other applicable documents, to NSA for approval. In addition to the items mentioned in paragraph **A2.6**, NSA also requires the following for COMSEC approval:

A2.3.1.1. **(AFMC)** List of all the COMSEC equipment and keys that will be accessed by the contractor (quantity, nomenclature title, version). Please include classification level of the keying material.

A2.3.1.2. **(AFMC)** Address the memo to: National Security Agency/Information Assurance Directorate Policy & Doctrine Division, 9800 Savage Road, Suite 6749, Fort George G. Meade, MD 20755-6749.

A2.3.1.3. **(AFMC)** See **Attachment 3** for a sample memo.

A2.4. (AFMC) Restricted Data (RD): Program Manager creates NID request memo; PEO signs memo; Contracting Officer sends memo to DSS; DSS sends memo to DOE for approval. Contracting Officer with help from the servicing IP Office sends a copy of the approved NID to SAF/AAZ.

A2.4.1. **(AFMC)** DSS requires a formal signed memorandum addressed to DOE requesting RD access. The memo must contain a description of the work to be done and the reason/justification why RD access is necessary. DSS will forward memo, along with all other applicable documents, to DOE for approval. See paragraph **A2.6** for the information needed in the memo and **Attachment 3** for a sample memo. DOE address: Headquarters Security Operations, Office of Resource Management & Mission Support, Office of Defense Nuclear Security, NA-72/Germantown Building, U.S. Department of Energy, 1000 Independence Avenue, SW, Washington, D.C. 20874-1207

A2.5. (AFMC) Top Secret: Program Manager creates NID package; Contracting Officer requests risk/vulnerability assessments from DSS; Contracting Officer, with assistance from the Program Manager and Unit Security Manager, sends NID package to PEO; PEO signs package and sends to OCA for approval (unless PEO is the OCA and then PEO approves NID); OCA approves NID; Contracting Officer, with assistance from the Program Manager and Unit Security Manager, sends NID approval to DSS. Contracting Officer with help from the servicing IP Office sends a copy of the approved NID to SAF/AAZ. See **Attachment 4** for a sample OCA Top Secret NID request package.

A2.5.1. **(AFMC)** DSS only requires a copy of the DD Form 254 and signed AF approved TS NID memo to update their databases. DSS will assist by providing copies of most recent risk/vulnerability assessments.

A2.5.2. **(AFMC)** If requesting DSS to propose TS NID or information is not owned by the AF, Program Manager creates NID request memo; PEO signs memo; Contracting Officer sends memo to DSS; DSS sends memo to OCA; OCA has 30 days to approve/disapprove and send back to DSS. Contracting Officer with help from the servicing IP Office sends a copy of the approved NID to SAF/AAZ.

A2.5.2.1. **(AFMC)** DSS requires a formal signed memorandum addressed to the OCA requesting TS access. The memo must contain a description of the work to be done and the reason/justification of why TS access is necessary. DSS will forward memo, along with all other applicable documents, to the OCA for approval. When DSS proposes the NID on behalf of the Contracting Officer, the AF will have 30 days to respond to DSS's proposal. If the AF doesn't answer within 30 days or contact DSS with justification prior to 30 days in the case of a potential denial, DSS will assume AF's concurrence on the NID and DSS will continue with the NID process. See paragraph **A2.6** for the information needed in the memo and **Attachment 3** for a sample memo.

A2.6. (AFMC) The Contracting Officer emails NID request memos to the DSS NID mailbox **NID@DSS.mil.** The following mailboxes are also available should correspondence require a higher classification: SIPR: **NID@dss.smil.mil** JWICS: **NID@dss.ic.gov.** All NID request memos should include:

A2.6.1. **(AFMC)** Memo signed by PEO.

A2.6.2. **(AFMC)** Name of Company; Address; Cage Code; Description of its foreign ownership

A2.6.3. **(AFMC)** Contract Number or Program Name or Project Name or Request for Proposal Number; period of performance

A2.6.4. **(AFMC)** DD Form 254; if for subcontractor, include prime contractor DD Form 254 also

A2.6.5. **(AFMC)** Description of the work the contractor is preforming

A2.6.6. **(AFMC)** Description of the technology to be accessed

A2.6.7. **(AFMC)** Justification of why the contractor needs access to the proscribe information

A2.6.8. **(AFMC)** Identify how the release of proscribed material is consistent with the national security interests of the U.S. Government.

A2.6.9. **(AFMC)** Industrial Security and Program Office points of contact.

Attachment 3 (Added-AFMC)

PROGRAM EXECUTIVE OFFICER NATIONAL INTEREST DETERMINATION REQUEST MEMORANDUM (SAMPLE)

Figure A3.1. Program Executive Officer National Interest Determination Request Memorandum (Sample).

MEMORANDUM FOR (Address for NSA or DOE)

FROM: (Office Symbol of Program Executive Officer)

SUBJECT: Request for Consideration of National Interest Determination (NID)

References:
(a) National Industrial Security Program: Procedures for Government Activities Relating to Foreign Ownership, Control or Influence (FOCI) (DoDM 5220.22, Vol 3)
(b) National Industrial Security Operating Manual (NISPOM) (DoD 5220.22-M, Para 2-309)
(c) Executive Order 12829, National Industrial Security Program

1. Pursuant to the above references, request favorable consideration in granting a National Interest Determination (NID) to FULL NAME / IDENTIFICATION AND ADDRESS OF COMPANY (complete identification to include all subcontractors, subsidiaries, partnerships, and full description of relationships/individual product lines, etc. shall be detailed in Tab "A" as outlined below).

2. The following justification and supporting data is provided for your review and consideration:
a. We request favorable consideration be given for the release of _____ _____ "proscribed information" (to include specific levels, etc.). In the enclosed attachments our request shall detail compelling evidence that release of such information to INSERT NAME OF COMPANY advances the national security interests of the United States.

3. The point of contact is Name, office symbol, unclassified email address, commercial and DSN phone numbers.

IRA M. SAMPLE
Program Executive Officer

Attachments:
Tab A - Name of Company; Address; Cage Code; Description of its foreign ownership
Tab B - Contract Number or Program Name or Project Name or Request for Proposal Number; period of performance
Tab C - Description of the work the contractor is preforming
Tab D - Description of the technology to be accessed

Tab E - Justification of why the contractor needs access to the proscribe information
Tab F - Identify how the release of proscribed material is consistent with the national security interests of the U.S. Government.
Tab G - Industrial Security and Program Office points of contact.
Tab H – DD Form 254; if for subcontractor, include prime contractor DD Form 254 also
Tab I – (for COMSEC) List of all the COMSEC equipment and keys that will be accessed by the contractor (quantity, nomenclature title, version); include classification level of the keying material.

Attachment 4 (Added-AFMC)

TOP SECRET NATIONAL INTEREST DETERMINATION (NID) REQUEST PACKAGE (SAMPLE)

Table A4.1. Top Secret National Interest Determination (NID) Request Package (Sample).

MEMORANDUM FOR OFFICE SYMBOL OF THE ORIGINAL CLASSIFICATION AUTHORITY OF THE COLLATERAL TOP SECRET INFORMATION

FROM: OFFICE SYMBOL OF REQUESTING GOVERNMENT CONTRACTING ACTIVITY (GCA)

SUBJECT: Request for Consideration of National Interest Determination (NID) (FOUO)

References:

(a) National Industrial Security Program: Procedures for Government Activities Relating to Foreign Ownership, Control or Influence (FOCI) (DoDM 5220.22, Vol 3)

(b) National Industrial Security Operating Manual (NISPOM) (DoD 5220.22-M, Para 2-309)

(c) Executive Order 12829, National Industrial Security Program

1. Pursuant to the above references, request favorable consideration in granting a National Interest Determination (NID) to FULL NAME / IDENTIFICATION AND ADDRESS OF COMPANY (complete identification to include all subcontractors, subsidiaries, partnerships, and full description of relationships/individual product lines, etc. shall be detailed in Tab "B" as outlined below).

2. The following justification and supporting data is provided for your review and consideration:

a. We request favorable consideration be given for the release of _____ _____ "proscribed information" (to include specific levels, etc.). In the enclosed attachments our request shall detail compelling evidence that release of such information to INSERT NAME OF COMPANY advances the national security interests of the United States.

3. The point of contact is Name, office symbol, unclassified email address, commercial and DSN phone numbers.

IRA M. SAMPLE
Contracting Officer

Attachments:

Tab A - Staff Summary Sheet – Coordination with Government PM, PCO, and PEO

Tab B - Identification of the proposed awardee(s) along with a synopsis of its foreign

ownership. Include solicitation/contract number/subcontract number, if applicable, and other reference numbers to identify the action.

(Full company identification & foreign ownership synopsis)

1. Full Company Identification:

a. Company Name: _____

b. FSC/CAGE Code: _____

c. Facility Clearance: _____

d. Physical Location (Street Address): _____

e. Is Corporate Headquarters same as Item "d" above: Yes ___ No ___

(1) If "No" - specify / list Corporate Headquarters information (Items "a" - "d" above).

_____

_____

f. Facility Clearance: _____

g. Product Line (relevant to this request; detail by location/activity and by subsidiary/subcontractor relationship, etc.): _____

h. Foreign Ownership Synopsis & Corporate Relationships: (detail all foreign ownership, partnerships, subsidiaries, affiliations - in addition to narrative; provide a linear organizational chart depicting all corporate entities/relationships, etc. DSS is your POC for this information.)

i. Provide a copy of the company's current Special Security Agreement: Obtain from Defense Security Service FOCI Operations Division.

(Note: All question/answer spaces above are not representative of allowable narrative - continue on additional pages to sufficiently detail)

Tab C - Procurement and performance requirements

Tab D - DD Form 254, if for subcontractor, include prime contractor DD Form 254 also

Tab E - Rationale for advancement of National Security interests. Identification of national security interests involved and the ways in which award of the contract helps advance those interests.

Tab F - Alternative means of satisfying requirements. Provide a description of any alternate means available to satisfy the requirement, and the reasons alternative means are not acceptable.

Tab G - Government's Counterintelligence Assessment/Foreign Ownership Issues. Defense Security Service FOCI office will help provide this information.

Tab H - Proposed NID Approval / Disapproval Letter

Apply appropriate classification/controlled unclassified information markings to all documents as applicable.